Codierungstheorie (Sommersemester 2014)

Irene Bouw, Michel Börner

Blatt: 04
Punkte: 10

Abgabe zu zweit **vor** der Vorlesung am Di., **20.05.14** um 10:15 Uhr im Raum E 20.

Aufgabe 8 (Erweiterte Codes)

Sei $\mathcal{C} \subset \mathbb{F}_2^n$ ein (n,k,d)-Code. Wir bezeichnen mit $\tilde{\mathcal{C}} = \psi(\mathcal{C})$ den um ein Paritätsbit erweiterten Code, wie definiert in Beispiel 1.6.3.(b) im Skript.

a) Zeige, dass $\tilde{\mathcal{C}}$ ein $(n+1,k,\tilde{d})$-Code mit der folgenden Prüfmatrix ist:

$$\tilde{H} = \left(\begin{array}{ccc|c} 1 & \cdots & 1 & 1 \\ \hline & & & 0 \\ & H_{\mathcal{C}} & & \vdots \\ & & & 0 \end{array}\right) .$$

b) Für welche d gilt $\tilde{d} = d+1$? (1+1 = **2 P**)

Aufgabe 9 (Duale Codes)

Gegeben sei der $(32,16)$ - Code $\mathcal{C}$ über $\mathbb{F}_2$ mit einer Erzeugermatrix von folgender Form

$$G := (I_{16} \mid A) \quad , \quad A = \left(\begin{array}{c|c|c|c} B & I_4 & I_4 & I_4 \\ \hline I_4 & B & I_4 & I_4 \\ \hline I_4 & I_4 & B & I_4 \\ \hline I_4 & I_4 & I_4 & B \end{array}\right) \quad , \quad B = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \quad , \quad I_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} .$$

a) Zeige, dass $\mathcal{C}$ selbstdual ist und gib eine Prüfmatrix für $\mathcal{C}$ an.

b) Zeige folgende Aussage für beliebige lineare Codes über $\mathbb{F}_2$.
Für Codewörter x, y eines selbstdualen Codes gilt: $4 \mid w(x) \quad \wedge \quad 4 \mid w(y) \quad \Longrightarrow \quad 4 \mid w(x+y)$,
wobei $w(\cdot)$ das Hamming-Gewicht bezeichnet.

c) Zeige, dass obiger Code $\mathcal{C}$ Minimaldistanz 8 hat.
Hinweis: Es darf ohne Beweis verwendet werden, dass die Summe von bis zu vier Spalten aus A mindestens Gewicht 4 hat.

(1,5+1+2 = **4,5 P**)

Aufgabe 10 (Endliche Körper)

Gegeben sei $f = x^3 + x + 1 \in \mathbb{F}_2[x]$. Schreibe $\alpha := x + (f)$ für die Restklasse von x.

a) Zeige, dass f irreduzibel über $\mathbb{F}_2$ ist und schließe, dass $K := \mathbb{F}_2[x]/(f)$ ein Körper ist.
(Zur Erinnerung: $\mathbb{F}_2[x]/(f) \simeq \{a_0 + a_1\alpha + a_2\alpha^2 \mid a_i \in \mathbb{F}_2\}$)

b) Bestimme die multiplikativen Inversen aller Elemente in $K^\times$ sowie deren Ordnung.

c) Prüfe, ob $g = x^4 - 2 \in \mathbb{F}_7[x]$ reduzibel ist und gib ggf. eine Zerlegung in irreduzible Faktoren an. (1+1,5+1 = **3,5 P**)